



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/623,488	10/30/2000	Feng Bao	P19949	7274

7055 7590 02/03/2004

GREENBLUM & BERNSTEIN, P.L.C.
1950 ROLAND CLARKE PLACE
RESTON, VA 20191

EXAMINER

PARTHASARATHY, PRAMILA

ART UNIT	PAPER NUMBER
----------	--------------

2136

DATE MAILED: 02/03/2004

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary

Application No.

09/623,488

Applicant(s)

BAO ET AL.

Examiner

Pramila Parthasarathy

Art Unit

2133

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133).
- Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☒ Responsive to communication(s) filed on 12 November 2002.
- 2a) ☐ This action is **FINAL**. 2b) ☒ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) ☒ Claim(s) 1-7 is/are pending in the application.
- 4a) Of the above claim(s) _____ is/are withdrawn from consideration.
- 5) ☐ Claim(s) _____ is/are allowed.
- 6) ☒ Claim(s) 1-7 is/are rejected.
- 7) ☐ Claim(s) _____ is/are objected to.
- 8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) ☒ The specification is objected to by the Examiner.
- 10) ☐ The drawing(s) filed on _____ is/are: a) ☐ accepted or b) ☐ objected to by the Examiner.
- Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
- Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. §§ 119 and 120

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some * c) ☐ None of:
- ☐ Certified copies of the priority documents have been received.
 - ☐ Certified copies of the priority documents have been received in Application No. _____.
 - ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).
- * See the attached detailed Office action for a list of the certified copies not received.
- 13) ☐ Acknowledgment is made of a claim for domestic priority under 35 U.S.C. § 119(e) (to a provisional application) since a specific reference was included in the first sentence of the specification or in an Application Data Sheet. 37 CFR 1.78.
- a) ☐ The translation of the foreign language provisional application has been received.
- 14) ☐ Acknowledgment is made of a claim for domestic priority under 35 U.S.C. §§ 120 and/or 121 since a specific reference was included in the first sentence of the specification or in an Application Data Sheet. 37 CFR 1.78.

Attachment(s)

- 1) ☒ Notice of References Cited (PTO-892)
- 2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
- 3) ☒ Information Disclosure Statement(s) (PTO-1449) Paper No(s) #6, #7, #8.
- 4) ☐ Interview Summary (PTO-413) Paper No(s). _____.
- 5) ☐ Notice of Informal Patent Application (PTO-152)
- 6) ☐ Other: _____.

DETAILED ACTION

1. Claims 1 – 7 are presented for examination

Specification

The disclosure is objected to because of the following informalities:

- d) "the second party accepts the second digital data" (page 5 Line
- 3). Examiner interprets as "the second party accepts the first digital data".

Appropriate correction is required.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

2. Claim 1 is rejected under 35 U.S.C. 103(a) as being unpatentable over Micali (U.S. Patent No. 5,666,420) in view of Angebaud et al. (U.S. Patent No. 5,218,637).

As per Claim 1, Micali discloses

a) the first party encrypting the first digital data and generating an authentication certificate, the authentication certificate authenticating that the encrypted first digital data is an encryption of the first digital data, and sending certificate to the second party (Col.5 Lines 46 – 48);

b) the second verifying that the encrypted first digital data is an encryption of the first digital data using the authentication certificate, and the second party sending the second digital data to the first party if the verification is positive (Col.9 Lines 50 – 51);

c) the first party verifying that the second digital data is valid, and if the verification is positive, the first party accepts the second digital data and sends the unencrypted first digital data to the second party (Col.5 Lines 52 – 54);

d) the second party verifying that the first digital data is valid, and if the verification is positive, the second party accepts the first digital data (Col.5 Lines 55 – 60); otherwise, the second party sends the encrypted first digital data and the second digital data to a third party, having a decryption key to decrypt the encrypted first digital data (Col.5 Lines 60 – 62); and

e) the third party decrypting the encrypted first digital data to obtain the first digital data, verifying that the first and the second digital data are valid and, if both the first and the second digital data are verified as valid, sending the first digital data to the second party and the second digital data to the first party (Col.5 Lines 63 - 67).

Micali does not explicitly disclose that the first party sending the unencrypted first digital data after the first party verifies that the second digital data from the second party

is valid. However, in an analogous environment, Angebaud discloses a method of exchanging digital data between a first party having a unique first digital data and a second party having a unique second digital data over a communication link (Col.1 Lines 12 – 14) and also discloses the method comprising a – d (Col.9 Lines 29 – 51).

- a) the first party sending the encrypted first digital data to the second party;
- b) the second party verifying that the encrypted first digital is an encryption of the first digital data and second party sending the second digital data to the first party;
- c) the first party verifying that the second digital data is valid and sends the unencrypted first digital data to the second party;
- d) the second verifying that the first digital data is valid, accepts the first digital data.

Therefore, it would have been obvious to a person of ordinary skill in the art to implement the claimed invention by including a method for sending the unencrypted first digital data after establishing the trust there by to eliminate the need to decrypt the first digital data. Such modifications would have been obvious because by combining the teachings of Micali with Angebaud, the second party has no need to decrypt the first digital data thereby saving time in decrypt algorithm computation.

As per Claim 2, Micali discloses

the first party in step a) encrypting the first digital data on a concatenation of file M_A and a one-way hash of file M_B (Col.8 Lines 59 – 64 and Col.5 Lines 58 – 59); and

the second party in step b) if the verification is positive, encrypting the second digital data on a concatenation of file M_B and a one-way hash of file M_A (Col.8 Lines 59 – 64 and Lines 50 – 51).

As per Claim 3, Micali discloses

Wherein the first and second digital data are digital signatures belonging to the first and second party, respectively (Col.4 Line 66 and Col.3 Lines 62 – 63 and Col.4 Lines 14 – 34).

As per Claim 4, Micali discloses

the second digital data is a file M which the first party wishes to receive from the second party in exchange for the first digital data (Col.5 Lines 46 – 53). Micali does not explicitly disclose that the file M is a secret file. However, Angebaud discloses

Wherein the second digital data is a secret file M which the first party wishes to receive from the second party in exchange for the first digital data (Col.1 Lines 12 – 14 and Col.9 Lines 34 – 61). It would have been obvious to a person of ordinary skill in the art to interpret the second digital data is a secret file, as it is well known in the art that digital signature scheme is based on secret key cryptography.

As per Claim 5, Micali discloses

Wherein the first party has a pair of public/private keys in a first digital signature scheme (Col.10 Lines 55 – 58);

The second party has a pair of public/private keys in a second digital signature scheme (Col.10 Lines 61 – 65); and

The third party has a pair of public/private keys in a public key encryption scheme (Col.10 Lines 50 – 54).

As per Claim 6, Micali discloses

Wherein the digital signature schemes are discrete logarithm based schemes; and the public key encryption is a discrete logarithm based scheme (Col.10 Lines 50 – 54).

As per Claim 7, Micali discloses

the public key encryption scheme is a discrete logarithm based scheme (Col.10 Lines 50 – 54).

Micali does not disclose the digital signature schemes are Guillou-Quisquater type digital signature schemes. However, Angebaud discloses

Wherein the digital signature schemes are Guillou-Quisquater type digital signature schemes (Col.7 Lines 24 – 68 and Col.8 Lines 1 – 45). Therefore, it would have been obvious to a person of ordinary skill in the art to implement the claimed invention by including a method for using the Guillou-Quisquater digital signature schemes there by eliminating the need to transfer a secret and/or controlling an action between two parties which establish reciprocal authentication, without a previously shared secret and without a common cryptographic algorithm. Such modifications would

have been obvious because by combining the teachings of Micali with Angebaud, the first and second parties can keep the parallel accreditations in each exchange to an absolute minimum.

Conclusion

3. Any response to this action should be mailed to:

Commissioner of Patents and Trademarks, Washington, D.C. 20231 or
faxed to: (703) 872-9306 for all formal communications.

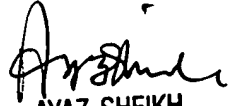
Hand-delivered responses should be brought to Crystal Park II, 2121 Crystal
Drive, Arlington, VA, Fourth Floor (Receptionist).

Any inquiry concerning this communication or earlier communications from the
examiner should be directed to Pramila Parthasarathy whose telephone number is 703-
305-8912. The examiner can normally be reached on 8:00a.m. To 5:00p.m..

If attempts to reach the examiner by telephone are unsuccessful, the examiner's
supervisor, Albert Decady can be reached on 703-305-9595. The fax phone number for
the organization where this application or proceeding is assigned is 703-872-9306.

Any inquiry of a general nature or relating to the status of this application or
proceeding should be directed to the receptionist whose telephone number is 703-305-
3900.

Pramila Parthasarathy
Patent Examiner
Art Unit 2133
703-305-8912
January 30, 2004.


AYAZ SHEIKH
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100